O que caracteriza uma moeda?

Ouro

- É aceito amplamente e reconhecido como moeda;
- Sua dificuldade (física) de mineração o torna raro;
- Alto custo de extração;
- O mercado não pode ser inundado de ouro;

Criptomoeda

- Também precisa ser aceita e reconhecida;
- O algoritmo deve fazer com que sua mineração também seja um processo difícil;
- Alto custo de mineração (hardware, energia) que varia conforme o valor da moeda;
- O programa não pode deixar o mercado não ser inundado pela criptomoeda;

O que são criptomoedas?

Dinheiro Comum

- Emitido e controlado pelo Banco Central;
- Dependente do governo;
- Podem ser armazenadas em bancos;
- Deve ser declarado para o governo;
- Aceitado somente em dimensão local;
- Taxado;
- Seu roubo é crime;
- Relativamente estável;

Criptomoeda

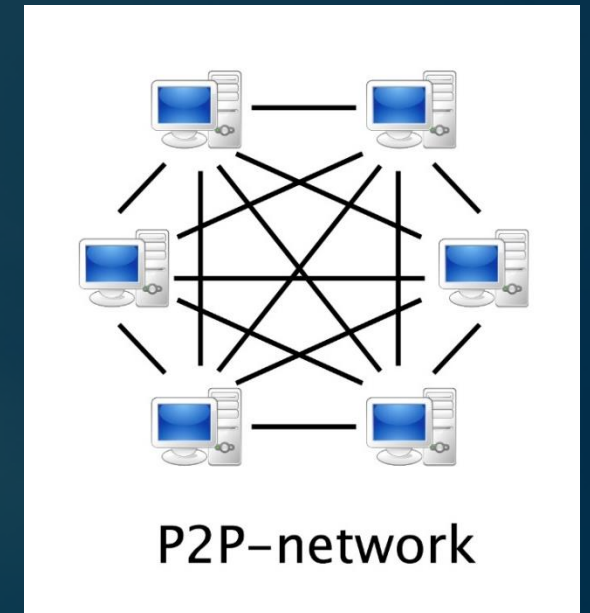
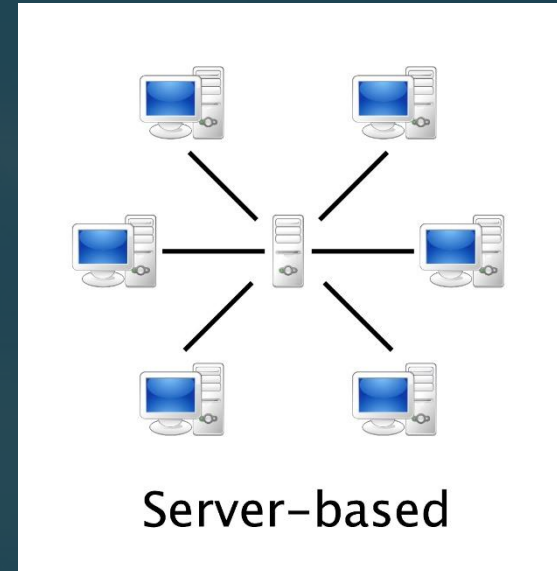
- Não possui autoridade responsável;
- Autônoma, gerida por um algoritmo;
- Armazenadas somente em carteiras criptografadas;
- Anônima, apesar do código-fonte e das transações serem públicas;
- Global;
- Sem impostos;
- Não há a quem recorrer em caso de roubo;
- Instável;

Como são produzidas?

- O algoritmo da moeda virtual é criado normalmente por uma equipe de programas anônimos.

- Um programa P2P (e de código aberto) e lançado no ar, com a finalidade de gerenciar todos os processos que envolvem a moeda virtual.

- Ele controla a dificuldade de mineração da moeda, emissão de novas hashes e outros fatores relacionados.

- Caso a moeda se torne popular, o algoritmo irá tornar sua mineração mais difícil, e os próprios usuários atribuirão seu valor, conforme leis de mercado.

Quais criptomoedas existem?

All ▾ | Currencies ▾ | Assets ▾ | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$ 6,355,940,521	$ 415.19	15,308,400 BTC	$ 90,785,600	-1.54 %	
2	Ethereum	$ 1,044,352,041	$ 13.44	77,703,030 ETH	$ 45,055,300	18.11 %	
3	Ripple	$ 297,557,136	$ 0.008728	34,090,841,338 XRP *	$ 1,996,550	-1.48 %	
4	Litecoin	$ 149,167,080	$ 3.32	44,875,776 LTC	$ 1,308,480	-1.83 %	
5	MaidSafeCoin	$ 48,882,901	$ 0.108016	452,552,412 MAID *	$ 578,526	0.78 %	
6	Dash	$ 32,066,375	$ 5.10	6,289,621 DASH	$ 284,844	-2.90 %	
7	Dogecoin	$ 24,570,667	$ 0.000238	103,448,036,649 DOGE	$ 202,571	-1.82 %	
8	Factom	$ 21,147,502	$ 2.42	8,753,250 FCT *	$ 1,682,180	3.02 %	
9	BitShares	$ 20,256,298	$ 0.007953	2,546,914,475 BTS *	$ 2,528,710	-5.78 %	
10	Stellar	$ 13,044,014	$ 0.002378	5,485,679,598 XLM *	$ 144,710	-10.63 %	
11	Monero	$ 12,988,917	$ 1.15	11,279,704 XMR	$ 218,734	2.17 %	

Cerca de 700 moedas, de acordo com o CoinMarketCap.

Mineração de Criptomoedas

1. O algoritmo precisa de pessoas para verificar todas as transações feitas na rede. Caso contrário, não seria possível efetuá-las;

2. Mineradores devem verificar escrever essas transações num bloco público, trabalho que é recompensado com criptomoedas;

3. Tais mineradores também tentam “adivinhar” a hash utilizada na criptografia de tal bloco. O vencedor também é recompensado com criptomoedas;

4. A dificuldade de mineração é constantemente ajustada com base na quantidade de mineradores, potência de seus equipamentos, entre outros fatores;

ac9b5974f7ab490f26...	5.405 BTC
498bb062c30412575...	0.413 BTC
2a6e49d1de08f0498...	1.762 BTC
9d5f6f531d9a2dd8fb...	0.025 BTC
0f9fe7922c526045fb...	0.196 BTC
5fe15cabe9d508b9fa...	5.563 BTC

Transações criptografadas e escritas num bloco público pelos mineradores.

0000003b8eea63ac9845e3754a7c3a43 ✗
000000230b5bb673f55bc2dbdfdc113df ✗
00000031e6176d583bd0323ecc688e77 ✗
000000499e62f5715af39f90c337e1ba0 ✓
0000001f790779d1bc364244a2f71cf7e ✗
00000003bdf305e33732d6d5b5b31800 ✗

Tentativas de encontrar a hash correspondente a cada bloco, o que requer milhões de cálculos por segundo.

Como começar a usar criptomoedas?

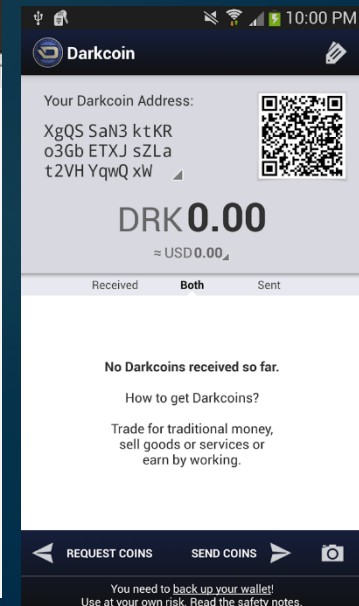
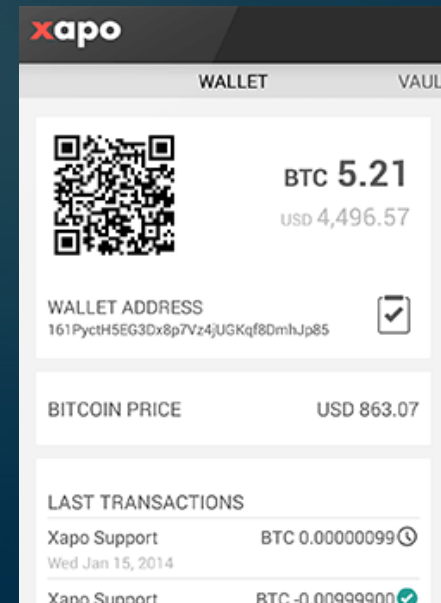
1 – Decidir a moeda que irá usar.

- Finalidade na qual pretende usá-la;
- Dificuldade de mineração;
- Lastro;
- Aceitabilidade/Popularidade;
- Segurança;
- Riscos envolvendo a moeda;
- Histórico de instabilidade, variações de mercado.

2 – Visitar os sites do projeto.

- Se familiarizar com a terminologia;
- Verificar a dificuldade de mineração;
- Onde comprar;

3 – Instalar uma carteira.

- Fazer o download de uma wallet, instalar e esperar sua sincronização;
- Usar uma wallet temporária online, para as primeiras transações;
- Ao final da sincronização, você estará apto a realizar transações;

Como conseguir criptomoedas?

✓ Comprar

- Existem sites que convertem moeda local em criptomoeda;
- Vendendo bens ou serviços;
- Criptomoeda é uma forma de dinheiro como qualquer outra;

✓ Faucets

- Sites que oferecem criptomoedas de graça;
- Normalmente uma pequena quantidade a cada período de tempo;
- Não costuma ser instantâneo;
- Pouco lucrativo;

✓ Mineração

- Possui custos como equipamento próprio e energia;
- Sua rentabilidade varia conforme a moeda;
- É necessário considerar diversos fatores e fazer as contas antes de partir para a mineração;
- Pode ser feita solo ou em equipe;
- O equipamento utilizado pode ser uma placa gráfica (GPU), um processador (CPU) ou ASIC (hardware específico para a função – como é o caso das Bitcoins);

Formas de Mineração

✓ Configuração Básica

- Pesquisar os requisitos para a mineração da sua criptomoeda;
- Decidir entre minerar com GPU, CPU ou ASIC.
- Cada criptomoeda usa um algoritmo diferente para mineração. É necessário verificar qual hardware se dá melhor com tal algoritmo;
- Decidir entre mineração solo ou em grupo.
- Baixar um programa minerador. Esses programas variam conforme o seu hardware (tipo e marca), então é preciso decidir o tipo de mineração primeiro.
- Configurá-lo e iniciar a mineração.

1 – Mineração Solo

- Tende a se tornar inviável com a popularização da moeda;
- Recompensas instantâneas e inteiras, porém menores – já que um computador sozinho realiza menos cálculos;
- Utiliza um servidor solo;

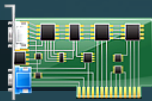
2 – Mineração em Grupo

- Escolher uma pool de mineração, que será responsável por enviar os blocos;
- O poder de todos os computadores é repartido, e suas recompensas também;
- É preciso ter determinado saldo para receber a recompensa;
- Pode ser taxado;
- Podem haver pools públicas;

Formas de Mineração

1 – Mineração com CPU

- Usa o cpuminer;
- Normalmente mais lenta;
- Consome menos energia;
- Depende do processador;

2 – Mineração com GPU

- Usa o CUDAMiner para NIVIDIA, e SGMiner para AMD, entre outros;
- Mais indicado para PC's gamers;
- É necessário ficar atento as especificações máximas de temperatura e voltagem;
- Não é possível realizar tarefas que exijam processamentos gráficos avançados durante a mineração;

✓ Configuração Final

- Baixar o programa escolhido conforme sua necessidade;
- Configurar um arquivo .bat para inicializa-lo, informando detalhes como sua carteira, servidor da pool, potência e outros argumentos;
- Começar a mineração e ficar atento aos resultados obtidos;

Terminologia

Coin: unidade da moeda virtual;

Wallet: carteira virtual, onde seu saldo é armazenado;

Core: realiza a mesma função que a wallet, mas também faz com que seu computador se torne um node integrante da rede P2P;

Wallet Online: carteira online, porém menos segura;

Sincronização: processo no qual todas as transações da moeda são baixadas e verificadas, para atualizar a carteira;

Moeda imatura: unidade que acabou de ser minerada, e precisa primeiro ser conferida para depois usada;

Miner: programa utilizado para mineração;

Pool: servidor responsável por enviar blocos para os mineradores. Existem servidores compartilhados ou solo, cada um com suas respectivas taxas;

Escrow: espécie de "seguradora" de criptocoins;

Algoritmo: forma pela qual os blocos são encriptados. Exemplos: x11, sha256, scrypt;

Currency: cotação da moeda;

Fee: taxa cobrada para intermédio da moeda por uma pool, por exemplo;